ハイブリッドモードの技術動向調査

株式会社レピダム

2020 年 12 月

本評価結果の概要（エグゼクティブサマリー）

2017 年から量子安全もしくは量子耐性のある暗号アルゴリズム（Post Quantum Cryptography, 以下、PQC）の標準化/選定が NIST などの組織において実施されている。この標準化/選定の終了後に実際のサービスや製品などへの適用には多くの時間がかかってしまうことが想定される。実際にすでに標準化されている暗号技術は、選定後サービスや製品への適用までに 10 年弱 *の年月を要している。従来の現代暗号から PQC への移行やシステムマイグレーションをした上で、新しい技術が浸透するまでには長期間必要であり、このタイムラグを緩和するための利用方法として「ハイブリッドモード」という概念が注目されている。このハイブリッドモードとは、従来の暗号技術と PQC を組み合わせることで、新しい技術である PQC が普及するまでの時間を確保できる効果や、従来の暗号技術の利用を規定している標準化仕様/ガイドラインにおいても、PQC を利用できるメリットがあると考えられる。しかしながら、ハイブリッドモードの目的や導入する背景、また、安全性に関する学術的なアプローチによる研究に関する情報が整理されていない。本調査では、ハイブリッドモードを導入する目的や背景を把握するために、ハイブリッドモードに関係することが期待される標準化団体やその組織の動向調査を実施した。また、現時点でハイブリッドモードを構成する際に想定されている PQC アルゴリズム及び、標準化動向や OSS などの実装状況に関する調査を実施した。

- ハイブリッドモードの標準化動向
  - IETF の tls WG において、TLS 1.3 でハイブリッドモードを利用可能にするための Internet Draft である「Hybrid key exchange in TLS 1.3」が、Working Group の検討項目として採択され、重要なテーマとしてコンセンサスが得られている。
  - Open Quantum-Safe プロジェクトにおいて、NIST の標準化会議で候補として残っているほぼ全ての PQC アルゴリズムが実装されており、TLS や SSH などのプロトコルで動作させる環境が準備されている。
- ハイブリッドモードで利用可能となるアルゴリズム候補
  - NIST が主催している標準化会議で候補として残っている PQC アルゴリズムは実装されており、それらのアルゴリズムを OpenSSL などに実装され、実際の世の中で利用されている TLS プロトコルや SSH プロトコルでの実現可能性が確認されている。いくつかの PQC アルゴリズムにおいてはデータサイズに関する問題が発生している。
  - ハイブリッドモードは、鍵交換とデジタル署名での利用が想定されており、ハイブリッド鍵交換については学術的な研究成果も発表されている。
- 各標準化団体・組織でのハイブリッドモードの取り扱い
  - ハイブリッドモードの導入に関する背景や目的について、明確に言及/定義している標準化団体・組織はなかったが、この調査を通して明らかになったことは以下のとおりである。
    - ✧ 従来の暗号技術と比較すると、PQC アルゴリズムへの安全性評価の実績や歴史が浅いため、PQC アルゴリズムにおける脆弱性の発見は社会へのインパクトを軽減する。そのため、ハイブリッドモードで利用している暗号アルゴリズム（従来の暗号技術または PQC アルゴリズム）のいずれかが安全であれば、セキュリティが最低限担保されることが期待できること。

---

* 認証付き暗号である Galois/Counter Mode （GCM） を暗号スイートとして利用するために規定された TLS 1.2 （2008 年 8 月に RFC として発行）が、実際に運用されているサーバやブラウザの 80%程度で TLS 1.2 が利用できるようになったのが 2016 年 9 月頃であるため、8 年の年月がかかっている。

- ✧ 標準化やソフトウェア/ハードウェアへの実装するためのバッファ期間としてのアルゴリズムの移行やシステムマイグレーションとしての役割が期待できること

・ ハイブリッドモードに関する安全性及び評価
  - 本調査の範囲において、ハイブリッドモードの構成法による安全性への実影響が報告された情報は発見されなかった。
  - ハイブリッドモードによって実現される安全性レベルは、従来の暗号アルゴリズムと PQC アルゴリズムで強い方の安全性は少なくとも達成できると考えられる。現在のところ、それ以上の安全性を達成しうるのかどうかは明らかになっていないと考えられる。

目次

1　はじめに

近年、重要な情報や通信における機密性、整合性、信頼性、否認防止などのセキュリティ要件を実現するために暗号技術は必須技術になっている。しかし、量子コンピュータの登場により、公開鍵暗号やデジタル署名を含む現在利用している暗号技術の多くは安全性が損なわれることが予想されている。

このような状況を考慮して、2017 年から量子安全もしくは量子耐性のある暗号アルゴリズム（Post Quantum Cryptography, 以下、PQC）の標準化/選定が NIST などの組織において実施されている。この標準化/選定の終了後に実際のサービスや製品などへの適用には多くの時間がかかってしまうことが想定される。実際にすでに標準化されている暗号技術は、選定後サービスや製品への適用までに 10 年弱の年月を要している。従来の現代暗号から PQC への移行やシステムマイグレーションをした上で、新しい技術が浸透するまでには長期間必要であり、このタイムラグを緩和するための利用方法として「ハイブリッドモード」という概念が注目されている。このハイブリッドモードとは、従来の暗号技術と PQC を組み合わせることで、新しい技術である PQC が普及するまでの時間を確保できる効果や、従来の暗号技術の利用を規定している標準化仕様/ガイドラインにおいても、PQC を利用できるメリットがあると考えられる。しかしながら、ハイブリッドモードの目的や導入する背景、また、安全性に関する学術的なアプローチによる研究に関する情報が整理されていない。本調査では、ハイブリッドモードを導入する目的や背景を把握するために、ハイブリッドモードに関係することが期待される標準化団体やその組織の動向調査を実施する。また、現時点でハイブリッドモードを構成する際に想定されている PQC アルゴリズム及び、標準化動向や OSS などの実装状況に関する調査を実施する。これらの調査により、ハイブリッドモードの導入する目的や背景などを明らかにする。

2　ハイブリッドモードとは

本章では、ハイブリッドモードがどのようなものなのかを明らかにするために、表 1 に示した、過去から暗号技術の検討を行なっている標準化団体・組織における「ハイブリッドモード」に関する調査を実施した。

項番	組織名	URL
1	National Institute of Standards and Technology (NIST)	https://www.nist.gov/
2	Internet Engineering Task Force (IETF)	https://www.ietf.org/
3	National Security Agency (NSA)	https://www.nsa.gov/
4	Cloud Security Alliance (CSA)	https://cloudsecurityalliance.org/
5	International Organization for Standardization（ISO）	https://www.iso.org
6	European Telecommunications Standards Institute (ETSI)	https://www.etsi.org/
7	PQCRYPTO	https://pqcrypto.eu.org/
8	Institute of Electrical and Electronics Engineers (IEEE)	https://standards.ieee.org/
9	International Telecommunications Union (ITU)	https://www.itu.int/
10	ANSI Accredited Standards Committee X9	https://x9.org/
11	Open Quantum-Safe (OQS)	https://openquantumsafe.org/

表 1 調査対象組織

調査対象の組織に対して網羅的な調査を実施することが理想的ではあるが、そのような調査方法を実施するにはかなり多くの時間を要してしまうため、以下に示すような調査方法によって効率的に調査を実施した。

- 調査方法
  - 表 1 に示した URL に対して、次に示す「調査キーワード」を指定して、検索結果として抽出された内容を確認して「ハイブリッドモード」に関する情報が含まれているかどうかを確認する
- 調査キーワード
  - ハイブリッドモードを取り扱う際に使用されると考えられるキーワードとして、以下に示すものを抽出している
    - ✧ Hybrid, Quantum, Crypto

2.1 各組織でのハイブリッドモードの取り扱い

本節では、暗号技術の標準化や利用について検討している主要な組織での「ハイブリッドモード」という考え方をどのように取り扱っているかどうかを調査した結果を示す。

2.1.1 National Institute of Standards and Technology (NIST)

NIST(米国国立標準技術研究所)は、米国の国立計量標準研究所である。ミッションは「経済保障を強化し生活の質を高めるよう科学的測定方法、標準、技術を改善し、米国の技術革新及び産業競争力を強化すること」となっている。進歩の著しい産業分野において、米国における技術評価ツールの提供など、各分野の成長・発展を技術面からサポートしている機関である。

現在、NSIT では PQC 標準化会議を開催しており、PQC アルゴリズムの評価を行なっている。ただし、ハイブリッドモードでの安全性評価などはスコープに入っていない。

また、PQC に関する情報発信が多く行われており、NISTIR 8105 Report on Post-Quantum Cryptography[†]という公式な資料が公開されている。今回の調査の目的であるハイブリッドモードに関する公式資料について調査したが、ハイブリッドモードについて言及している資料は調査の範囲では存在していなかったが、PQC 標準化会議において、「Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH」という発表 [1]が行われている。この発表は、AWS、Microsoft Research、Waterloo 大学によって投稿されており、当該発表の「2. Hybrid modes」において、ハイブリッドモードの目的について言及している。その目的としては「利用されるコンポーネントが一つでも壊れていない限り、期待されたセキュリティプロパティを確保すること」という記述程度に留まっており、具体的な定義を行われているようなものではない。しなしながら、「2.1 Goals for hybrid modes」という節の中で、その中でいくつかの目的(図 1)が示されている。この中で注目すべき項目としては、「利用されるコンポーネントが一つでも壊れていない限り、期待されたセキュリティプロパティを確保すること」と「Backwards compatibility(下位互換性)」が重要なポイントであると考える。

[†] https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

2.1 Goals for hybrid modes

The primary goal of a hybrid mode is to ensure that the desired security property holds as long as one of the component schemes remains unbroken. For key exchange, this means that the session key should remain secure (and thus application data confidential) as long as one of the component key exchange mechanisms is unbroken. For authentication, this means that the protocol should provide secure authentication as long as one of the digital signatures schemes is unbroken at the time of session establishment.

In addition to the primary cryptographic goals, there may be several additional goals for hybrid modes in real-world network protocols. These include:

Backwards compatibility. Clients and servers who are "hybrid-aware", i.e., compliant with whatever hybrid mode is added to TLS or SSH, should remain compatible with endpoints and middle-boxes that are not hybrid-aware.

The three scenarios to consider are:

1. Hybrid-aware client, hybrid-aware server: These parties should negotiate and use hybrid modes.
2. Hybrid-aware client, non-hybrid-aware server: These parties should negotiate a traditional (non-PQ) ciphersuite (if the hybrid-aware client is willing to downgrade to traditional-only).
3. Non-hybrid-aware client, hybrid-aware server: These parties should establish a traditional (non-PQ) ciphersuite (if the hybrid-aware server is willing to downgrade to traditional-only).

Ideally backwards compatibility should be achieved without extra round trips and without sending duplicate information; see below.

High performance. Use of hybrid modes should not be prohibitively expensive in terms of computational performance. In general this will depend on the performance characteristics of the specific cryptographic algorithms used, and the hybridization should not substantially affect performance. Preliminary results about such performance include [8, 9, 10].

Low latency. Use of hybrid modes should not substantially increase the latency experienced to establish a connection. Factors affecting this may include the following:

- The computational performance characteristics of the specific algorithms used. See above.
- The size of messages to be transmitted. Public key / ciphertext / signature sizes for post-quantum algorithms range from hundreds of bytes to over one hundred kilobytes, so this impact can be substantial. See [8, 9] for preliminary results in a laboratory setting, and [29] for preliminary results on more realistic networks.
- Additional round trips added to the protocol. See below.

No extra round trips. Attempting to negotiate hybrid modes should not lead to extra round trips in any of the three hybrid-aware/non-hybrid-aware scenarios listed above.

No duplicate information. Attempting to negotiate hybrid modes should not mean having to send multiple cryptographic values for the same algorithm.

図 1 ハイブリッドモードの目的

2.1.2 Internet Engineering Task Force (IETF)

IETF は、インターネットに関する技術仕様の標準化を推進および策定する機関であり、インターネットによってコンピュータシステムを相互に接続することを目的として、共通の技術仕様策定を議論することから発展した組織である。IETF でまとめられた技術文書は Request For Comments（RFC）と呼ばれており、これらの文書はワーキンググループを単位にして推進される。IETF における技術仕様策定の特徴は、ラフコンセンサス（Rough Consensus）とランニングコード（Running Code）とされており、まず、大まかな仕様を作成し、それから相互接続実験や実運用を通じて、工夫や改善を加

えながら仕様を実装していくという、非常に柔軟な仕様策定プロセスを有していることが特徴的な組織である。

IETF には、研究的なテーマについて検討する Internet Research Task Force (IRTF) があり、その中に暗号技術について検討を行う Crypto Forum Research Group (cfrg) があるが、PQC 自体の評価は IETF としては実施せずに NIST の評価結果を確認するという方針であるため、具体的な議論はされていない。しかし、実社会で利用されている通信プロトコルである IPsec、TLS、SSH などのハイブリッドモード利用について、Internet Draft が投稿され、議論されている。

ここで、実際に投稿されている Internet Draft であるハイブリッド鍵交換に関する「Post-quantum public key algorithms for the Secure Shell (SSH) protocol[‡]」を取り上げる。このドキュメントにおいてハイブリッドモードの直接的な説明はないが、「This document defines hybrid key exchange methods based on classical ECDH key exchange and post-quantum key encapsulation schemes.」とハイブリッド鍵交換について書かれている。また文中で「A hybrid key exchange method maintains the same level of security provided by current key exchange methods, but also adds quantum resistance. The security provided by the individual key exchange scheme in a hybrid key exchange method is independent. This means that the hybrid key exchange method will always be at least as secure as the most secure key exchange scheme executed as part of the hybrid key exchange method.」と書かれている。この部分を踏まえてハイブリッドモードについて整理すると「従来の暗号技術によって達成されている安全性レベルに PQC の性質を付与することを期待しており、それぞれのアルゴリズムで独立した処理するのではなく、どちらかが安全性レベルを達成できない状態になっていずれかのアルゴリズムによって守られることが担保されるような構成法」であることが示されている。

2.1.3 National Security Agency (NSA)

NSA は、米国国防総省の情報機関である。この組織における暗号技術との関わり合いは、NIST の前身である NBS が公募した標準暗号アルゴリズムの策定やハッシュ関数である Secure Hash Algorithm（SHA）シリーズ（ただし、SHA-3 は NIST の公募により選定）の開発にも大きく関わっている組織である。

NSA の公式サイトには、「Post-Quantum Cybersecurity Resources」というページが存在しているが、ハイブリッドモードに関する記述はなく、以下に示す項目についての情報公開が主目的であると考える。

- NSA’s Cybersecurity Perspective on Post-Quantum Cryptography Algorithms
- NSA’s Cybersecurity perspective on quantum key distribution and quantum key cryptography

2.1.4 Cloud Security Alliance (CSA)

CSA[§]は、クラウドコンピューティングでのセキュリティ保証を提供するためのベストプラクティスを促進し、クラウドコンピューティングに関する教育を提供して、クラウドセキュリティを実現することを目的として持つ非営利組織である。CSA には、Quantum Safe Security WG[**]が存在しており、物理学に基づいて鍵を安全に配送する技術である量子鍵配送（Quantum Key Distribution、以下 QKD）や PQC によってデータ保護するための量子安全な方式を暗号技術の専門家ではない一般の人た

[‡] https://datatracker.ietf.org/doc/draft-kampanakis-curdle-pq-ssh/

[§] https://cloudsecurityalliance.org/

[**] https://cloudsecurityalliance.org/research/working-groups/quantum-safe-security/

ちが理解するのに役立つように、情報発信および啓発することを目的としている。そのため、ハイブリッドモードの観点から見ると、スコープからやや外れていると考えられる。
また、Quantum Safe Security WG は、「The State of Post Quantum Cryptography」[2]や「Applied Quantum-Safe Security」[3]というドキュメントを発行しているが、その中で NIST や IETF と言った組織の紹介を行っており、実際の適用例としてハイブリッド鍵交換に関する動向を示している。

2.1.5 International Organization for Standardization（ISO）

国際標準化を行う ISO と IEC の合同委員会（ISO/IEC JTC 1）において、情報セキュリティに関する標準化を担当する副委員会である SC27 の WG 2"Cryptography and security mechanisms"において、暗号技術に関する標準化活動が行われている。
ISO は単独のアルゴリズムの標準化を目的としていて、ハイブリッドモードはスコープ外と考えられる。

2.1.6 European Telecommunications Standards Institute (ETSI)

ETSI は、ヨーロッパにおける通信関係の標準化機関であり、通信関係の EN（欧州規格）や ETS（欧州通信規格）を制定している。
ETSI では、Quantum-Safe Cryptography (QSC) working group という組織を有している。この WG は学術的な暗号研究と量子アルゴリズム研究の現状および実世界での展開に対する産業界の要件の両方を考慮して、量子安全な通信プロトコルの構成法とその実装を評価し、推奨することを目的としている。
QSC WG では、PQC の実用的な実装に焦点を当て、性能、実装能力、プロトコル、ベンチマーク、特定のアプリケーションのための実用的なアーキテクチャを考慮すると記載している。この WG の目的は暗号プリミティブの開発ではないことが明言されている。

2.1.7 PQCRYPTO

EU の Horizon 2020 における「Post-Quantum Cryptography for Long-Term Security」プロジェクトがある。このプロジェクトは3年間の期間で実施されており、その中でいくつかの報告書が発行されている。
その中で発行された報告書である「Post-Quantum Cryptography for Long-Term Security D5.2 Standardization: Final report」[4]において、ハイブリッドモードに関する記述がいくつか記述されているので、注目すべき箇所を以下に抜粋する。（図 2、図 3）

以下に示した図 2 において、ハイブリッドモードについて説明が行われている。この説明の中で、ハイブリッドモードとは「PQC と従来の暗号アルゴリズムの両方から作られる方式」とされている。具体的な構成法として、2 つのデジタル署名で構成されており、どちらか一方のデジタル署名を検証するのではなく両方のデジタル署名を検証するが必要であることを意味している。このアプローチは少なくともどちらかの方式が安全である限りセキュリティが担保されることを保証していると説明されている。

[2] "Hybrid Mode" algorithms are created from both, a post-quantum algorithm and an established pre-quantum algorithm. For example, a digital signature consists of two signatures, which both must be verified. This approach guarantees security as long as at least one scheme is secure. That way, the introduction of new schemes does not harm security.

図 2 ハイブリッドモードに関する説明

また、以下に示した図 3 において、「Selection criteria for quantum-safe hybrid cryptography」について説明されている。ここでは、ハイブリッドのコンセプトとして、従来の鍵交換アルゴリズムで PQC のための ephemeral な鍵で保護された秘密なマテリアルを交換し、その秘密のマテリアルを Key Derivation Function (KDF)に含めることによって、"harvest-then-decrypt"攻撃に対して保護された認証鍵確立を実現する」ことが示されている。

なお、"harvest-then-decrypt"攻撃とは、「日常的に暗号化されたデータを収集しておき（harvest）、量子コンピュータでの解読が現実的になった際に、harvest 期に収集した暗号データを解読する攻撃」のことである。このような攻撃に対して、ハイブリッドモードでの利用をしておくことで、従来の暗号アルゴリズムが量子コンピュータで解読されてしまったとしても、PQC によって保護されることを意味している。

- **Selection criteria for quantum-safe hybrid cryptography**
  The *quantum-safe hybrid* concept is a modular approach, allowing any authenticated key establishment mechanism to be protected against "harvest-then-decrypt" attacks by exchanging additional secret material protected with an ephemeral key for a quantum-safe public key cryptographic algorithm and including that secret material in the Key Derivation Function (KDF) run at the end of the key establishment protocol. Such an approach has been proposed for TLS in [27]. A current Internet-Draft provides a guideline to criteria for selecting public key encryption algorithms approved for experimental use in the quantum safe hybrid setting [26].

図 3 量子安全なハイブリッド暗号に関する選定基準

2.1.8 Institute of Electrical and Electronics Engineers (IEEE)

IEEE は、米国に本部を置く電気・情報工学分野の学術研究団体、技術標準化機関である。暗号技術での活動としては、公開鍵暗号のための標準化プロジェクトである IEEE 1363 やストレージ暗号化のためのプロジェクトである IEEE 1619 などが知られている。

IEEE は学術的研究団体である側面もあるため、ハイブリッドモードに関する学術論文は存在していたが、今回の標準化機関として注目した。その結果、ハイブリッドモードについて言及されているような情報は見当たらなかった。

2.1.9 International Telecommunications Union (ITU)

ITU は、電気通信に関する国際標準の策定を目的とした組織で、1947 年から国連の組織として運営されている。主に、電波の国際的な分配や混信防止のための国際的な調整、電気通信のグローバルな標準化の促進、開発途上国に対する技術援助の促進などの活動を推進している。

ITU において、セキュリティに関する議論は ITU-T SG17 で行われているが、主に議論されているテーマとして、QKD に関するものが多い印象を受けたが、PKI や X.509 証明書でのハイブリッドモードの話題が寄書や報告書の中で触れられている程度であった。

2.1.10 ANSI Accredited Standards Committee X9

ANSI は、1918 年に設立された米国の代表的な標準化機関であり、標準化規格の作成自体は実施せずに、他公認標準機関（ASO: Accredited Standards Organization）で作成された規格案の審議を行い、米国国家規格（ANSI 規格）として制定する組織である。
「Quantum Computing Risks to the Financial Services Industry」という報告書 [††]の中で、ハイブリッドモードとして鍵共有とデジタル署名での構成を行うことは、ハイブリッドモードを構成する方式に問題があった際の対策として効果的であることが書かれた文章があった。（図 4）

> At present, the future harvest & decrypt style attacks may be mitigated by deploying hybrid classical/quantum-safe cryptosystems. The idea behind hybrid cryptosystems is to combine a classical cryptographic algorithm with a quantum-safe cryptographic algorithm in the same system or subsystem. Hybridization is particularly attractive for key establishment and digital signatures. A hybrid signature scheme might combine a classical and a quantum-safe signature algorithm so that both signatures must be verified for the signature to be accepted. A hybrid key establishment protocol might derive a key from secret materials produced by both a classical and a quantum-safe algorithm.

図 4 ANSI X.9

2.1.11 Open Quantum-Safe (OQS)

OQS は、耐量子暗号の発展とプロトタイピングをサポートすることを目的としたオープンソースプロジェクトである。このプロジェクトは、PQC アルゴリズムのための C 言語の OSS である liboqs と、このプロトタイプをプロトコルやアプリケーションへの統合（広く利用されている OpenSSL ライブラリを含む）を主要な目的としている。
このプロジェクト自体が多くの PQC アルゴリズムを実装かつ公開しているので、実装的な観点から実際のプロトコルで動作させた際の問題点や課題について多くの知見を有していると考える。
このプロジェクトの主要な目的にもあるように、このプロジェクトで実装したプロトタイプを IETF で標準化されている通信プロトコルへの適用を行なっており、ハイブリッドモードに関する実装が公開されている。
以下に、公開されているハイブリッドモード構成を含むプロジェクト [‡‡]としては、TLS、SSH、X .509、CMS and S/MIME、External users of OQS が存在する。以下にいくつかピックアップして概要を示す。

- List of all supported QSC Signature / Key Exchange algorithms
  - 概要

[††] https://x9.org/wp-content/uploads/2019/03/X9_Quantum-Computing-Risk-Study-2019-02-14-finalS1.pdf
[‡‡] https://openquantumsafe.org/applications/

- IETF に Internet Draft を投稿している「Hybrid key exchange in TLS 1.3」[5]をベースにハイブリッド鍵交換を実現し、サーバ証明書では PQC を利用して相互接続性のテストを実施している。
- URL
  - https://test.openquantumsafe.org/

・ Benchmarking post-quantum cryptography in TLS
- 概要
  - PQC アルゴリズムは、従来の公開鍵アルゴリズムと比較して計算が遅い、公開鍵や暗号文/署名、もしくは両方が大きいという様々なトレードオフがある。それら単独でのパフォーマンスの測定は比較的容易ではあるが、現実的なネットワーク条件でのパフォーマンスに関する調査研究はあまり行われていないことに注目して、Linux カーネルのネットワーク機能を使用してネットワーク条件をエミュレートすることにより、TLS での実験を安価に実行するためのフレームワークを開発して利用している。
  - このテスト環境を使用することで、リンク遅延やパケット損失率などの変数を個別に制御し、さまざまな PQC アルゴリズム、特にハイブリッド鍵交換および PQC デジタル署名の TLS 接続確立パフォーマンスへの影響を調べることができる。
  - 実験の主な結果として、3～5%を超えるパケット損失率が、unstructured lattices に基づくものなど、多くのパケットにわたってフラグメント化する PQC アルゴリズムに大きな影響を及ぼし始めていることがわかります。
  -
- URL
  - https://openquantumsafe.org/research/PQCrypto-PaqSteTam20

・ CMS and S/MIME
- 概要
  - OpenSSL をフォークした実装では、PQC やハイブリッドデジタル署名を用いて S/MIME や CMS の署名を行うことができる。
  - X.509 形式で PQC やハイブリッドモードでのデジタル署名を利用できるように拡張している。なお、利用できるアルゴリズム一覧[§§]も公開されている。
- URL
  - https://openquantumsafe.org/applications/smime.html
  - https://openquantumsafe.org/applications/x509

OQS は、これだけのハイブリッドモードについて実装や実験を行なっているプロジェクトではあるが、ハイブリッドモード自体に関する言及している情報については、本調査の範囲では発見することができなかった。

2.2 本調査を踏まえて整理したハイブリッドモード

本節では、前節で調査したハイブリッドモードの現状を踏まえて、本動向調査としてハイブリッドモードについて、以下に示す 3 つの観点から整理を行う。

・ ハイブリッドモードが必要とされている理由は何か？
- 安全性に関する懸念（従来の暗号アルゴリズム）

[§§] https://github.com/open-quantum-safe/openssl#authentication

- ✧ 量子コンピュータが現実的になった時には、従来の暗号アルゴリズムは暗号技術としての要件を満たすことができなくなる。そのため、従来の暗号アルゴリズムと PQC アルゴリズムを組み合わせて利用することにより、従来の暗号アルゴリズムでは達成できなかった安全性を全体として量子コンピュータにも耐えうる安全性まで引き上げる

➢ 安全性に関する懸念（PQC アルゴリズム）

- ✧ PQC に完全移行した場合、PQC アルゴリズムは従来の暗号アルゴリズムと比較して量子コンピュータに耐性はあるが、従来の暗号アルゴリズムと比較して安全性評価手法などが成熟していないことや、製品やサービスに実装された PQC アルゴリズムが従来の暗号アルゴリズムと比較して様々な利用方法や攻撃に晒されていないことによる未知の脆弱性などのリスクが考えられる。

➢ 運用上の懸念

- ✧ 実社会での新しいアルゴリズム（PQC）やプロトコルの社会実装を行うと、ネットワーク上に配置されている機器が対応していないと通信できない。このような状況を回避するために「下位互換性」を実現することで古い機器で通信を行うことができる。
- ✧ 現行の FIPS140 などの認証プログラムは従来の暗号アルゴリズムのみに対応している。一方、NIST が行っている PQC 標準化会議は PQC アルゴリズム単体のみを評価しているため、実際に利用しようとすると利用できる製品や環境がない状況を生み出してしまう。

・ ハイブリッドモードに何を期待しているのか？

➢ 上記のような背景を踏まえて、ハイブリッドモードで利用している暗号アルゴリズムのどちらかが安全性に問題があったとしても、1 つでも無事なアルゴリズムによってセキュリティが最低限担保されることへの期待ができること。

➢ 標準化やソフトウェア/ハードウェアへの実装するためのバッファ期間としてのアルゴリズムの移行やシステムマイグレーションとしての役割が期待できること。

・ ハイブリッドモードの適用先はどのような領域か？

➢ 暗号プリミティブとしては「鍵交換」と「デジタル署名」でのハイブリッドモードでの利用が有望であると多くの組織が述べている。

- ✧ 例示としてあげられているのが、IETF で標準化されている TLS や SSH などの従来の暗号アルゴリズムを用いて鍵交換を行っている部分に対して PQC アルゴリズムを用いたハイブリッドモード向けの拡張を行いながら既存プロトコルの仕様との互換性を意識している。

➢ ハイブリッドモードでの利用が促進されることで、実際の環境で PQC が利用されるため利用時の課題や懸念事項などを洗い出すことができる。

3　ハイブリッドモードで利用可能となるアルゴリズム候補

本章では、ハイブリッドモードを構成する際に利用される PQC アルゴリズムについて、調査を行なった結果を示す。

主にハイブリッドモードで利用可能な PQC アルゴリズムについて、正式な文書として発行する組織は、現在 PQC 標準化会議を行なっている NIST や実社会で利用する通信プロトコルを標準化している IETF があるが、IETF では独自にハイブリッドモードで利用する PQC アルゴリズムを選定することはせずに、NIST の標準化会議の結果を踏まえて標準化していく方針であると考える。

以上のことから、ハイブリッドモードで利用可能な PQC アルゴリズムの候補としては、NIST の標準化会議で選ばれたアルゴリズムになると考える。

3.1　具体的なハイブリッドモード構成例：PQC アルゴリズム

実利用という観点で考えると、現在利用されている通信プロトコルは、従来の暗号アルゴリズムを前提に設計されているため、どのような影響が存在するのかをすべて抽出することが困難である。これは、PQC アルゴリズムと現行の暗号アルゴリズムを組み合わせて利用するハイブリッドモードについても同様の影響が予想される。このような状況を考慮して、実社会での利用を視野に入れた実験的な活動を先進的に実行した Google を参考にしながら Amazon AWS [6]、Microsoft Research [7]や Cloudflare [8]などが実証実験を行い調査結果の報告を行なっている。

多くの PQC アルゴリズムやハイブリッドモードに関する研究結果など多くが投稿されているが、ここでは、NIST 2nd Post-Quantum Cryptography Standardization Conference 2019. で発表された“Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.” [1]を取り上げる。これによって、実際に利用されているインターネットプロトコルである TLS 1.2 / 1.3 や SSH への影響を確認することができる。この論文において、メジャーな OSS である OpenSSL や OpenSSH に対して、PQC およびハイブリッドモードに関する実装を行ない、その影響を報告している 。(図 5、図 6)

その報告において、15 種類の PQC アルゴリズムに対する動作結果について整理されているので、全体を俯瞰したい場合には参照することをお勧めする。結果としては多くの PQC アルゴリズムが正常動作しているため、本調査では不具合が発生したケースについて抽出する。どのケースが正しく動作しなかったかについては、図中にある以下に抜粋した記号で動作しなかった理由が示されている。

◓ ： 正常動作させるために実装のパラメータを変更することで修正可能であり、プロトコル仕様には準拠している障害

○ ： 正常動作させるための修正がプロトコル仕様に違反する。または、まだ特定されていない理由による障害

不具合が発生したケースについて概要を整理すると、その原因は「プロトコルで定められているハンドシェイクで許容されているメッセージサイズが大きい」（例：TLS 1.3 における NTS-KEM） や「プロトコル仕様で許容されているメッセージサイズではあるが、原因不明なエラーが発生してしまうなどの問題が発生」するようなものである。このような不具合を引き起こしてしまった PQC アルゴリズムで NIST の標準化会議の Round 3 Finalist に選ばれているアルゴリズムは、鍵交換では Classic McEliece（NTS―KEM は Round 3 において、Classic McEliece としてマージされた。）、デジタル署名として Rainbow となる。この事実から得られる教訓としては、NIST の標準化会議での Round 3 Finalist に選ばれているようなアルゴリズムであってもアルゴリズム特性により鍵サイズやメッセージサイズなどが実社会で利用されている通信プロトコルに影響を与えてしまうような状況になっており、それらのアルゴリズムを利用する際に制約が与えられるケースがあることに注意することが必

要であると考える。なお、具体的なエラーを発生させたメッセージサイズなどについては、文献 [1] の「3.1.4 Lessons learned」で示されている。

	s2n (TLS 1.2)	**OpenSSL 1.0.2** (TLS 1.2)	**OpenSSL 1.1.1** (TLS 1.3)	**OpenSSH**
BIKE1-L1 (round 1)	– ●	●●	●●	●●
BIKE1-L3 (round 1)	– –	●●	●●	●●
BIKE1-L5 (round 1)	– –	●●	●●	●●
BIKE2-L1 (round 1)	– –	●●	●●	●●
BIKE2-L3 (round 1)	– –	●●	●●	●●
BIKE2-L5 (round 1)	– –	●●	●●	●●
BIKE3-L1 (round 1)	– –	●●	●●	●●
BIKE3-L3 (round 1)	– –	●●	●●	●●
BIKE3-L5 (round 1)	– –	●●	●●	●●
FrodoKEM-640-AES	– –	●●	●●	●●
FrodoKEM-640-SHAKE	– –	●●	●●	●●
FrodoKEM-976-AES	– –	●●	●●	●●
FrodoKEM-976-SHAKE	– –	●●	●●	●●
FrodoKEM-1344-AES	– –	◓◓	◓◓	●●
FrodoKEM-1344-SHAKE	– –	◓◓	◓◓	●●
Kyber512	– –	●●	●●	●●
Kyber768	– –	●●	●●	●●
Kyber1024	– –	●●	●●	●●
LEDAcrypt-KEM-LT-12†	– –	●●	●●	●●
LEDAcrypt-KEM-LT-32†	– –	●●	●●	●●
LEDAcrypt-KEM-LT-52†	– –	●●	●●	●●
NewHope-512-CCA	– –	●●	●●	●●
NewHope-1024-CCA	– –	●●	●●	●●
NTRU-HPS-2048-509	– –	●●	●●	●●
NTRU-HPS-2048-677	– –	●●	●●	●●
NTRU-HPS-4096-821	– –	●●	●●	●●
NTRU-HRSS-701	– –	●●	●●	●●
NTS-KEM(12,64)†	– –	○○	○○	○○
LightSaber-KEM	– –	●●	●●	●●
Saber-KEM	– –	●●	●●	●●
FireSaber-KEM	– –	●●	●●	●●
SIKEp503 (round 1)	– ●	– –	– –	– –
SIKEp434	– –	●●	●●	●●
SIKEp503	– –	●●	●●	●●
SIKEp610	– –	●●	●●	●●
SIKEp751	– –	●●	●●	●●

図 5 TLS および SSH 実装における PQC およびハイブリッドモードでの鍵交換における実行結果

	OpenSSL 1.1.1 (TLS 1.3)	OpenSSH
Dilithium-2	●●	●●
Dilithium-3	●●	●●
Dilithium-4	●●	●●
MQDSS-31-48	◓◓	●●
MQDSS-31-64	◓◓	●●
Picnic-L1-FS	◓◓	●●
Picnic-L1-UR	◓◓	●●
Picnic-L3-FS	○○	●●
Picnic-L3-UR	○○	●●
Picnic-L5-FS	○○	●●
Picnic-L5-UR	○○	●●
Picnic2-L1-FS	●●	●●
Picnic2-L3-FS	◓◓	●●
Picnic2-L5-FS	◓◓	●●
qTesla-I (round 1)	●●	●●
qTesla-III-size (round 1)	●●	●●
qTesla-III-speed (round 1)	●●	●●
Rainbow-Ia-Classic†	◓◓	◓◓
Rainbow-Ia-Cyclic†	●●	●●
Rainbow-Ia-Cyclic-Compressed†	●●	●●
Rainbow-IIIc-Classic†	◓◓	○○
Rainbow-IIIc-Cyclic†	◓◓	○○
Rainbow-IIIc-Cyclic-Compressed†	◓◓	○○
Rainbow-Vc-Classic†	◓◓	○○
Rainbow-Vc-Cyclic†	◓◓	○○
Rainbow-Vc-Cyclic-Compressed†	◓◓	○○
SPHINCS+-{Haraka,SHA256,SHAKE256}-128f-{robust,simple}	◓◓	●●
SPHINCS+-{Haraka,SHA256,SHAKE256}-128s-{robust,simple}	●●	●●
SPHINCS+-{Haraka,SHA256,SHAKE256}-192f-{robust,simple}	◓◓	●●
SPHINCS+-{Haraka,SHA256,SHAKE256}-192s-{robust,simple}	◓◓	●●
SPHINCS+-{Haraka,SHA256,SHAKE256}-256f-{robust,simple}	◓◓	●●
SPHINCS+-{Haraka,SHA256,SHAKE256}-256s-{robust,simple}	◓◓	●●

図 6 TLS および SSH 実装における PQC およびハイブリッド署名による認証における実行結果

図 5 および 図 6 において、TLS や SSH を実現するための実装/サービスにおける各 PQC アルゴリズムを追加した際の PQC アルゴリズム単体およびハイブリッドモードでの動作について示している。なお、動作結果が 2 列で示されているが、左側の結果が単体での動作、右側の結果がハイブリッドでの動作結果を示している。この結果を踏まえると、正常動作しないケースは、PQC アルゴリズム単体やハイブリッドモードに影響されていないことから、特定の PQC アルゴリズムに起因することが予想される。また、PQC アルゴリズム単体で動作するアルゴリズムは、実験的ではあるがハイブリッドモードでも利用できることが期待される。

3.2 具体的なハイブリッドモード構成例：ハイブリッド鍵交換

ハイブリッドモードでの利用として実験的に利用されている構成方法は、大きく分けて「鍵交換」と「認証（デジタル署名）」である。ここでは、ハイブリッドモードにおける鍵交換の具体的な手順として、文献 [1]でも取り上げられている TLS 1.3 プロトコルにおける適用事例にフォーカスして説明を行う。

本節では、ハイブリッドモードでの鍵交換を説明するにあたり、はじめに鍵交換に注目して必要最低限の「TLS 1.3 としてのハンドシェイク」においてハイブリッドモードの導入により変更の影響がある箇所を明確にし、その部分においてどのような処理で従来の暗号技術と PQC アルゴリズムを組み合わせて TLS プロトコルで導出する Master Secret (MS) を生成するのか手順を示す。

＜TLS 1.3 としてのハンドシェイク（概要）＞

TLS 1.3 プロトコルにおけるハイブリッドモードの鍵交換が関係するプロセスは、ハンドシェイクにおける ClientHello と ServerHello でやり取りされる supported_groups および key_share である。（図 7）

これらの extension（拡張属性）において、supported_groups では、対応する鍵交換方式として複数の候補が示されており、また、key_share では ECDH などの公開鍵を送信している。なお、図 7 において、ハイブリッドモードが関係している箇所は、太字斜体となっている拡張属性が該当する。

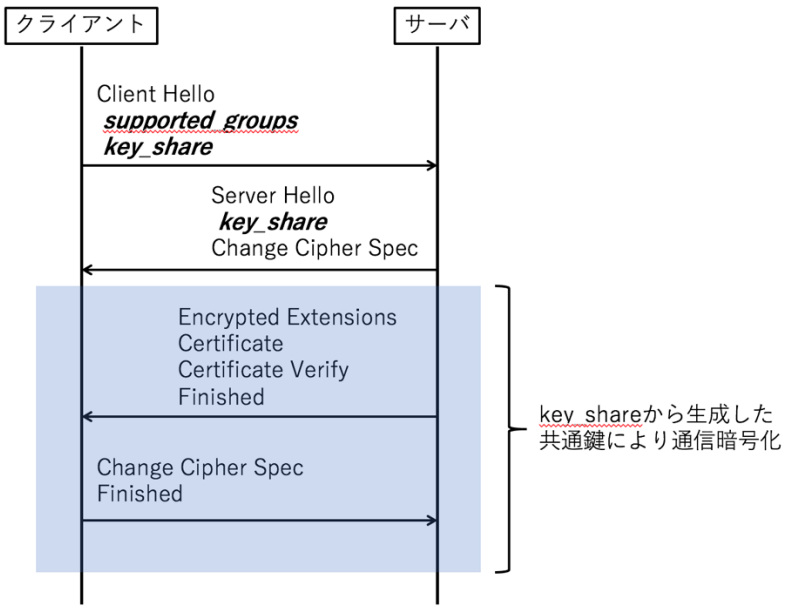

図 7 TLS 1.3 ハンドシェイク（概略）

図 7 において、太字斜体になっている箇所に対して、具体的なハイブリッドモードを把握できるよう、以下のような記号を定義して太字斜体部分を表現した。（図 8）

1. trad : 従来の暗号技術。TLS プロトコルにおいては、DHE や ECDHE
2. PQC : 耐量子計算機暗号アルゴリズム
3. $KeyGen_X() = (pk_X, sk_X)$: アルゴリズム X に関する鍵生成 (pk_X, sk_X)
4. cpk_X, csk_X : アルゴリズム X に関するクライアントの鍵ペア
5. spk_X, ssk_X : アルゴリズム X に関するサーバの鍵ペア
6. $Encaps_X(sk_X) = (ct_X, ss_X)$: アルゴリズム X による鍵カプセル化によって得られる暗号文 ct_X および共有秘密鍵 ss_X
7. $Decaps_Y(sk_Y, pk_Y) = ss_Y$: アルゴリズム Y による鍵カプセル化解除によって得られる共有秘密鍵 ss_Y
8. $HKDF(ss_{trad} \,||\, ss_{PQC}) = MS$: 従来の暗号技術により得られた共有秘密鍵 ss_{trad} および PQC により得られた共有秘密鍵 ss_{PQC} を連結した値を入力としたハッシュ関数ベースの鍵導出関数によって得られる MasterSecret（MS）

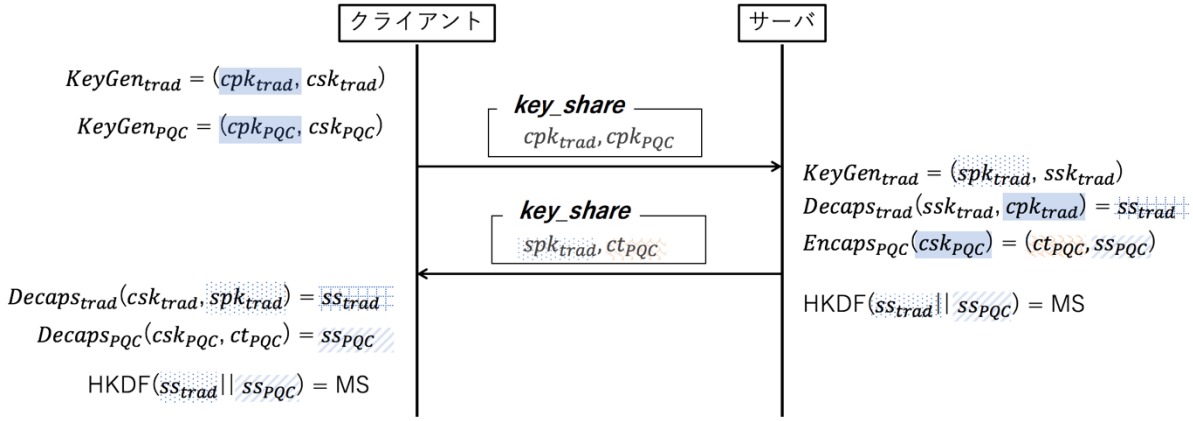

図 8 ハイブリッドモードにおける MasterSecret 生成

図 8 にあるように、クライアントがサーバへ送信する key_share を生成するタイミングで、PQC による鍵生成を行い、サーバは受信したクライアントの PQC 公開鍵を用いた暗号文によって PQC によるセッション鍵の共有を実現していることがわかる。

また、参考までに TLS 1.3 プロトコルにおける通常の鍵導出とハイブリッドモードを用いた鍵導出を比較した図を示す。（図 9、図 10）

参照している RFC や Internet Draft が異なるため表現が異なるが、HKDF への入力は青色でハッチングされた箇所がクライアントとサーバでやり取りをして生成した共有秘密鍵であることがわかる。

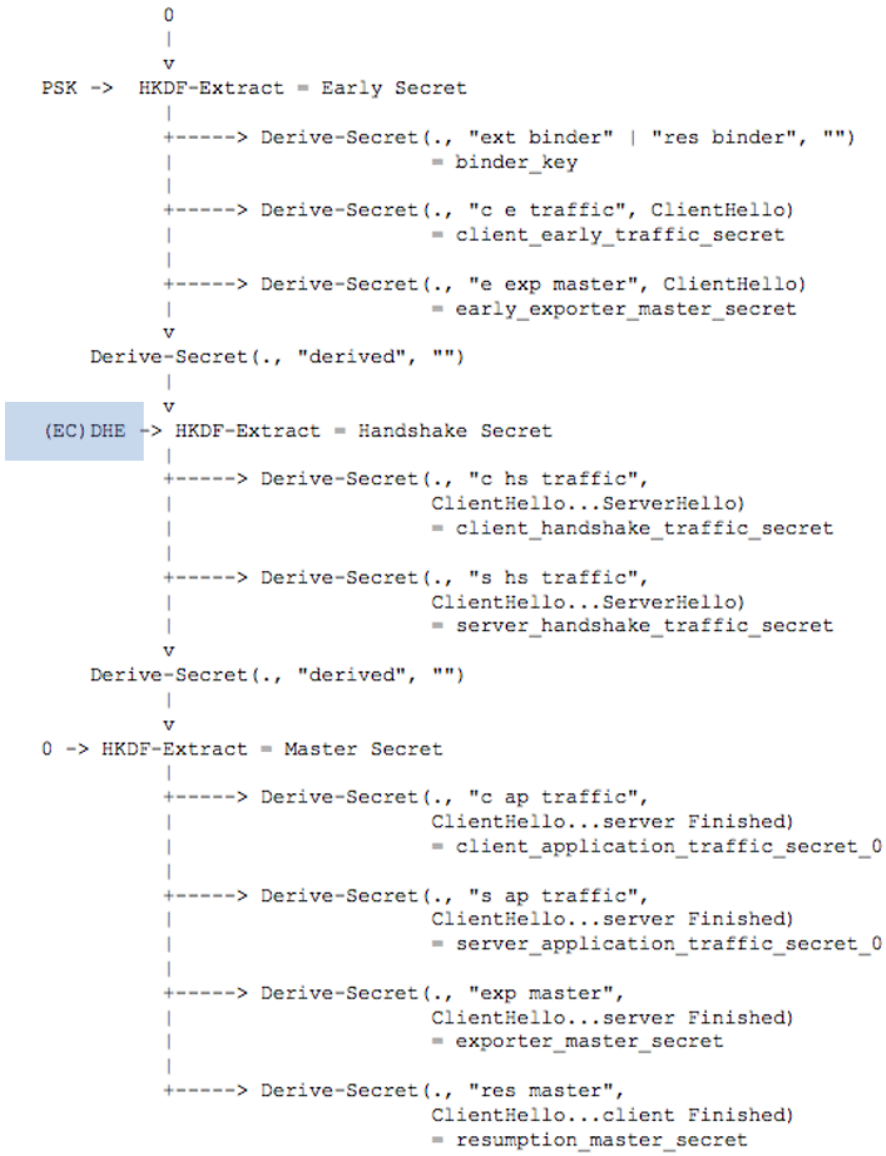

図 9 TLS 1.3 における鍵導出（通常の鍵導出）

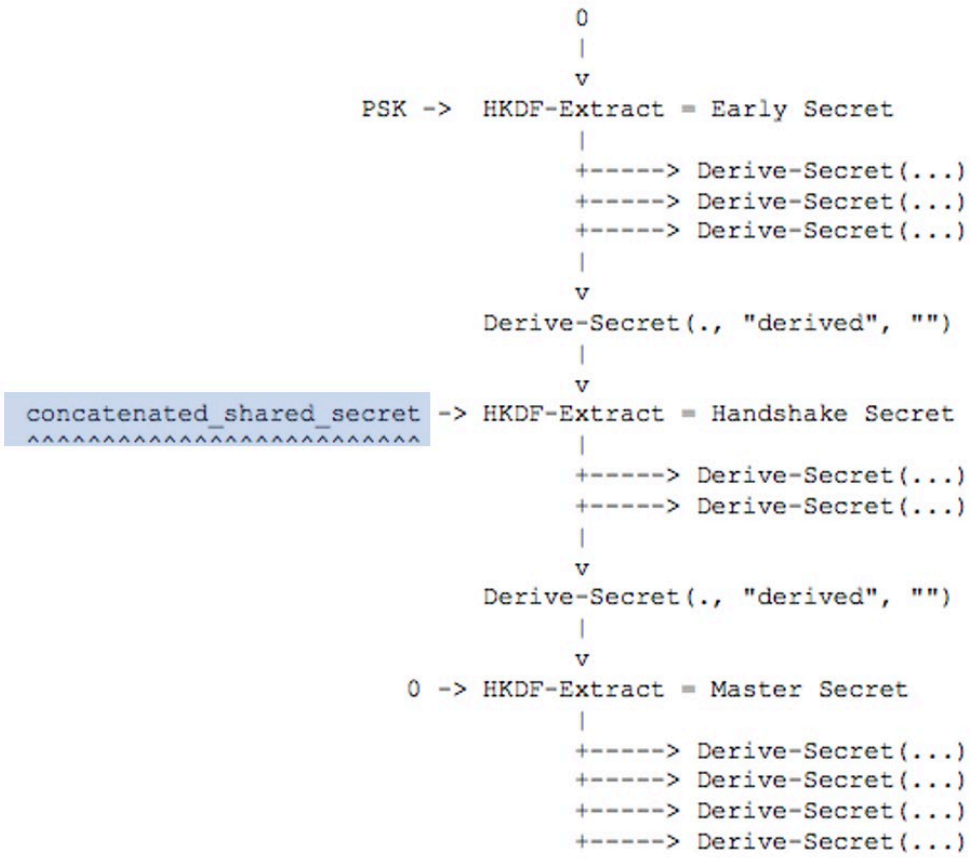

図 10 TLS 1.3 における鍵導出（ハイブリッドモード）

4　ハイブリッドモードの標準化動向

実社会においてハイブリッドモードが利用されるためには標準化されていることが望ましいと言える。本報告書では、実社会で暗号技術を利用しているプロトコルを標準化している IETF を中心にハイブリッドモードに関する標準化動向の調査を行なった結果を示す。

また、従来の暗号アルゴリズムから PQC アルゴリズムへの移行やシステムのマイグレーションを考慮したハイブリッドモードでの利用に耐えうるような利用可能な暗号ライブラリ環境として Open Quantum-Safe プロジェクトがあるため、そのプロジェクトでの実装状況についても調査結果を示す。

4.1　IETF での標準化動向

以下に、IETF における標準化動向を示す。

- Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography / 量子安全なハイブリッド暗号のための公開鍵暗号アルゴリズムの選択基準
  - 概要
    - Authenticated key exchange mechanisms instantiated with cryptosystems based on integer factorization, finite field discrete log, or elliptic curve discrete log, are

believed to be secure now but are vulnerable to a harvest-then-decrypt attack where an attacker who cannot currently break the mechanism records the traffic anyway, then decrypts it at some point in the future when quantum computers become available. The Quantum-safe Hybrid approach is a modular design, allowing any authenticated key exchange mechanism to be protected against the harvest-then-decrypt attack by exchanging additional secret material protected with an ephemeral key for a quantum-safe public key cryptographic algorithm and including that secret material in the Key Derivation Function (KDF) run at the end of the key exchange. This approach has been proposed in TLS as the Quantum-safe Hybrid handshake mechanism for Transport Layer Security protocol (QSH_TLS). This document provides a guideline to criteria for selecting public key encryption algorithms approved for experimental use in the quantum safe hybrid setting.

- ✧ この文書は、量子安全なハイブリッド環境での実験的使用が承認された公開鍵暗号アルゴリズムを選択するための基準のガイドラインを提供する。
  素因数分解問題、有限体上の離散対数問題、楕円曲線上の離散対数問題に基づく暗号システムでインスタンス化された認証付鍵交換メカニズムは、現在は安全であると考えられている。
  一方で、これらの現行暗号システムは、harvest-then-decrypt 攻撃と呼ばれる、攻撃者が現状安全とされる暗号化トラフィック情報を収集しておき、将来、量子計算機が利用可能になった際に、過去に収集した暗号化トラフィック情報を解析する攻撃に対しては脆弱である。
  量子安全なハイブリッドアプローチはモジュール設計であり、現行の認証付鍵交換を harvest-then-decrypt 攻撃から保護するために、量子安全な公開鍵暗号アルゴリズムで交換された秘密情報を、鍵交換の最後に実行される KDF(Key Derivation Function)に含める対策をとっている。このアプローチは、トランスポート層セキュリティプロトコル（QSH_TLS）の量子安全ハイブリッドハンドシェイク機構として TLS で提案されている。

- ➢ URL
  - ✧ https://datatracker.ietf.org/doc/draft-whyte-select-pkc-qsh/

・ Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS) / Transport Layer Security 1.2 (TLS) のための量子安全なハイブリッド鍵交換方式 (PQ KEM)

- ➢ 概要
  - ✧ Hybrid key exchange refers to executing two independent key exchanges and feeding the two resulting shared secrets into a Pseudo Random Function (PRF), with the goal of deriving a secret which is as secure as the stronger of the two key exchanges. This document describes new hybrid key exchange schemes for the Transport Layer Security 1.2 (TLS) protocol. The key exchange schemes are based on combining Elliptic Curve Diffie-Hellman (ECDH) with a post-quantum key encapsulation method (PQ KEM) using the existing TLS PRF.
  - ✧ この文書は、TLS 1.2 での利用に向けた量子安全なハイブリッド鍵交換方式(PQ KEM)を提案する IETF ドラフトである。
    ハイブリッド鍵交換とは、2 つの独立した鍵交換を実行し、その結果として得られる 2 つの共有秘密を 擬似ランダム関数(PRF)の入力とすることで、2 つの鍵交換のうちより安全性が高い方の鍵交換と同程度の安全性を持つ秘密情報を導き出すことを目的としている。本文書で提案する鍵交換方式は、既存の TLS PRF を用いて、楕円曲

線 Diffie-Hellman 鍵交換(ECDH)と量子安全な鍵カプセル化方式(PQ KEM)を組み合わせたものである。

- URL
  - https://datatracker.ietf.org/doc/draft-campagna-tls-bike-sike-hybrid/

- Post-quantum public key algorithms for the Secure Shell (SSH) protocol / Secure Shell (SSH) プロトコルのための量子安全な公開鍵アルゴリズム
  - 概要
    - This document defines hybrid key exchange methods based on classical ECDH key exchange and post-quantum key encapsulation schemes. These methods are defined for use in the SSH Transport Layer Protocol. It also defines post-quantum public key authentication methods based on post-quantum signature schemes. These methods are defined for use in the SSH Authentication Protocol.
    - この文書は、現行の ECDH 鍵交換と量子安全な鍵カプセル化方式に基づいたハイブリッド鍵交換方式を定義する IETF ドラフトである。これらの方式は SSH トランスポートレイヤプロトコルで使用するために定義している。また、量子安全な署名方式に基づく公開鍵認証方式も定義されており、SSH 認証プロトコルで使用することを目的とする。
  - URL
    - https://datatracker.ietf.org/doc/draft-kampanakis-curdle-pq-ssh/

- The Transition from Classical to Post-Quantum Cryptography / 現行暗号から量子安全な暗号への移行
  - 概要
    - Quantum computing is the study of computers that use quantum features in calculations. For over 20 years, it has been known that if very large, specialized quantum computers could be built, they could have a devastating effect on asymmetric classical cryptographic algorithms such as RSA and elliptic curve signatures and key exchange, as well as (but in smaller scale) on symmetric cryptographic algorithms such as block ciphers, MACs, and hash functions. There has already been a great deal of study on how to create algorithms that will resist large, specialized quantum computers, but so far, the properties of those algorithms make them onerous to adopt before they are needed. Small quantum computers are being built today, but it is still far from clear when large, specialized quantum computers will be built that can recover private or secret keys in classical algorithms at the key sizes commonly used today. It is important to be able to predict when large, specialized quantum computers usable for cryptanalysis will be possible so that organization can change to post-quantum cryptographic algorithms well before they are needed. This document describes quantum computing, how it might be used to attack classical cryptographic algorithms, and possibly how to predict when large, specialized quantum computers will become feasible.
    - この文書は、RSA や楕円曲線暗号などの現行暗号から、量子安全な暗号への移行に関して、量子計算機による現行暗号への攻撃方法や、現行暗号にとって壊滅的な影響を与える量子計算機がいつ実現可能になるかを予測する方法について説明する。
      量子計算とは、計算に量子的特徴を利用するコンピュータである。20 年以上前から、非常に大型で、特殊な量子計算機を作ることができれば、RSA や ECDSA、ECDH な

どの現行の非対称暗号アルゴリズムや、ブロック暗号、MAC、ハッシュ関数などの対称暗号アルゴリズムに、壊滅的な影響を与える可能性があることが知られていた。大型の特殊な量子計算機に対抗するアルゴリズムを構成する方法については、すでに多くの研究が行われている。しかし、現状、それらのアルゴリズムの特性から、現実的に必要とされる前の段階での採用は困難なものとなっている。現在では、小型の量子計算機が作られているが、一般的に使用されている鍵サイズで現行暗号の秘密鍵や秘密鍵を復元できるような、大型で特殊な量子計算機がいつ作られるかは、まだ明らかになっていない。暗号解析に使用可能な大型で特殊な量子計算機がいつ構築されるかを予測できることは重要であり、それにより、組織が必要とする前の段階で、量子安全な暗号アルゴリズムに変更することが可能となる。そこで、本文書では、量子計算機について説明し、現行暗号を攻撃するために量子計算機をどのように使用するか、また、現行暗号に壊滅的な影響を与える量子計算機がいつ登場するかを予測する方法について説明する。

- URL
  - https://datatracker.ietf.org/doc/draft-hoffman-c2pq/

また、今後の IETF におけるハイブリッドモードの標準化動向を把握したい際には、IETF が提供している「Datatracker[***]」を用いることで、数多く投稿されている Internet Draft を検索することができる。

4.2 Open Quantum-Safe での実装動向

以下に、Open Quantum-Safe Project における実装動向を示す。このプロジェクトの基本的な方針として、NIST が主催している Post-Quantum Cryptography Standardization で Round 3 Submissions に残っている Finalists や Alternate Candidates が実装対象とされているが、KEM では NTRU Prime、Signature schemes では GeMSS が 2020 年 12 月 1 日現在、実装はされていない[†††]。

表 2Open Quantum-Safe 実装アルゴリズム

項番	アルゴリズム種別	アルゴリズム名	
1	KEM	Classic McEliece	*Classic-McEliece-348864, Classic-McEliece-348864f, Classic-McEliece-460896, Classic-McEliece-460896f, Classic-McEliece-6688128, Classic-McEliece-6688128f, Classic-McEliece-6960119, Classic-McEliece-6960119f, Classic-McEliece-8192128, Classic-McEliece-8192128*

[***] https://datatracker.ietf.org/

[†††] https://openquantumsafe.org/liboqs/algorithms/

2		Kyber	Kyber512, Kyber768, Kyber1024, Kyber512-90s, Kyber768-90s, Kyber1024-90s
3		NTRU	NTRU-HPS-2048-509, NTRU-HPS-2048-677, NTRU-HPS-4096-821, NTRU-HRSS-701
4		SABER	LightSaber-KEM, Saber-KEM, FireSaber-KEM
5		BIKE	BIKE1-L1-CPA, BIKE1-L3-CPA, BIKE1-L1-FO, BIKE1-L3-FO
6		FrodoKEM	FrodoKEM-640-AES, FrodoKEM-640-SHAKE, FrodoKEM-976-AES, FrodoKEM-976-SHAKE, FrodoKEM-1344-AES, FrodoKEM-1344-SHAKE
7		HQC	HQC-128-1-CCA2, HQC-192-1-CCA2, HQC-192-2-CCA2, *HQC-256-1-CCA2*, *HQC-256-2-CCA2*, *HQC-256-3-CCA2*
8		SIKE	SIDH-p434, SIDH-p503, SIDH-p610, SIDH-p751, SIKE-p434, SIKE-p503, SIKE-p610, SIKE-p751, SIDH-p434-compressed, SIDH-p503-compressed, SIDH-p610-compressed, SIDH-p751-compressed, SIKE-p434-compressed, SIKE-p503-compressed, SIKE-p610-compressed, SIKE-p751-compressed
9	Signature	Dilithium	Dilithium2, Dilithium3, Dilithium4
10		Falcon	Falcon-512, Falcon-1024
11		Rainbow	Rainbow-Ia-Classic, Rainbow-Ia-Cyclic, Rainbow-Ia-Cyclic-Compressed, *Rainbow-IIIc-Classic, Rainbow-IIIc-Cyclic, Rainbow-IIIc-Cyclic-Compressed, Rainbow-Vc-Classic, Rainbow-Vc-Cyclic, Rainbow-Vc-Cyclic-Compressed*
12		Picnic	Picnic-L1-FS, Picnic-L1-UR, Picnic-L1-full, Picnic-L3-FS, Picnic-L3-UR, Picnic-L3-full, Picnic-L5-FS, Picnic-L5-UR, Picnic-L5-full, Picnic3-L1, Picnic3-L3, Picnic3-L5

13		SPHINCS+-Haraka	SPHINCS+-Haraka-128f-robust, SPHINCS+-Haraka-128f-simple, SPHINCS+-Haraka-128s-robust, SPHINCS+-Haraka-128s-simple, SPHINCS+-Haraka-192f-robust, SPHINCS+-Haraka-192f-simple, SPHINCS+-Haraka-192s-robust, SPHINCS+-Haraka-192s-simple, SPHINCS+-Haraka-256f-robust, SPHINCS+-Haraka-256f-simple, SPHINCS+-Haraka-256s-robust, SPHINCS+-Haraka-256s-simple
14		SPHINCS+-SHA256	SPHINCS+-SHA256-128f-robust, SPHINCS+-SHA256-128f-simple, SPHINCS+-SHA256-128s-robust, SPHINCS+-SHA256-128s-simple, SPHINCS+-SHA256-192f-robust, SPHINCS+-SHA256-192f-simple, SPHINCS+-SHA256-192s-robust, SPHINCS+-SHA256-192s-simple, SPHINCS+-SHA256-256f-robust, SPHINCS+-SHA256-256f-simple, SPHINCS+-SHA256-256s-robust, SPHINCS+-SHA256-256s-simple
15		SPHINCS+-SHAKE256	SPHINCS+-SHAKE256-128f-robust, SPHINCS+-SHAKE256-128f-simple, SPHINCS+-SHAKE256-128s-robust, SPHINCS+-SHAKE256-128s-simple, SPHINCS+-SHAKE256-192f-robust, SPHINCS+-SHAKE256-192f-simple, SPHINCS+-SHAKE256-192s-robust, SPHINCS+-SHAKE256-192s-simple, SPHINCS+-SHAKE256-256f-robust, SPHINCS+-SHAKE256-256f-simple, SPHINCS+-SHAKE256-256s-robust, SPHINCS+-SHAKE256-256s-simple

※ 表 2 において、斜体になっているアルゴリズムは、スタック使用量が多く、スレッドや制約のある環境での実行を行うと失敗する可能性がある。

5　ハイブリッドモード構成法に関する安全性

PQC アルゴリズム自体の安全性評価について、NIST が主催している PQC 標準化会議において実施されている。しかし、この会議のスコープが PQC に限定されているため、ハイブリッドモード構成法に関する安全性については評価対象外となっている。

以上のことから、本報告書では、ハイブリッドモードの構成法における安全性について評価行なっている事例があるか、また、実際にハイブリッドモードの構成法での安全性への影響があった事例があるかどうかの調査結果を示す。

5.1　ハイブリッドモードの構成法における安全性評価

ハイブリッドモードに対して、学術論文ではいくつかの研究成果が公開されている。ここでは、いくつかの学術論文を紹介する。なお、ハイブリッドモードによって実現される安全性レベルは、従来の暗号アルゴリズムと PQC アルゴリズムで強い方の安全性は少なくとも達成できると考えられる。現在のところ、それ以上の安全性を達成しうるのかどうかは明らかになっていないと考えられる。

- タイトル
  - Post-quantum key exchange for the TLS protocol from the ring learning with errors problem [9]
- 概要
  - R-LWE 問題に基づいた鍵交換を TLS プロトコルで利用するための暗号スイートを検討して、PQC 鍵交換の実用性を実証する。この論文の中では、従来の鍵交換と R-LWE 問題に基づいた鍵交換を置き換えただけではなく、ハイブリッドモードに関する実験も行われている。
- URL
  - https://eprint.iacr.org/2014/599.pdf

- タイトル
  - Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids [10]
- 概要
  - 一般的な Bellare-Rogaway モデルを拡張し、鍵交換プロトコルの故障回復力について検討している。また、一般的なハイブリッド鍵交換プロトコルのセキュリティを分析しており、この構成が主要な鍵交換方式の 1 つの故障に対する耐障害性をどのように確保しているかが示されている。
- URL
  - https://eprint.iacr.org/2017/1252.pdf

- タイトル
  - KEM Combiners [11]
- 概要
  - 鍵交換におけるハイブリッドモードで実現されている異なる KEM を組み合わせる構成方法に関する安全性について示されている。具体的には、単一の KEM に依存するのではなく、異なる KEM 構造を組み合わせることで安全な KEM を構成する KEM Combiners という概念であり、構成要素として任意の KEM のセットが与えられた時に、構成要素である KEM のうちの少なくとも一つが安全である限り（CCA）安全な新しい KEM を構成できることが示されている。

- URL
  - https://eprint.iacr.org/2018/024.pdf

- タイトル
  - Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange [12]
- 概要
  - 従来の暗号技術から PQC への移行する方法についての研究が促進されている中で、一般的なセキュリティを保証するための 1 つのアプローチとして、従来の暗号技術と PQC アルゴリズムを組み合わせたハイブリッドモードによる鍵交換プロトコルがあるが、ハイブリッド鍵交換プロトコルに関する設計とセキュリティに関する実証という観点から適切な理論的アプローチが欠落していることが指摘されている。この論文の中で異なるシナリオにおいても区別できるようにするための KEM に関するセキュリティに関する考え方、TLS1.3 でハイブリッド鍵交換を実現するためのハイブリッド KEM を構築するためのいくつかの組み合わせ方法、また、KEM をビルディングブロックとして使用するハイブリッド鍵交換のための構成方法が提示されている。
- URL
  - https://eprint.iacr.org/2018/903.pdf

また、本調査の範囲において、ハイブリッドモードの構成法による安全性への実影響が報告された情報を発見できなかった。

6　まとめ

本報告書では、PQC を議論していることが想定される 11 つの組織を対象にハイブリッドモードに対してどのようなアプローチを取っているのかを調査を行った。その結果としてハイブリッドモードについて、以下に示すようなことが明らかにできた。

- ハイブリッドモードが必要とされている理由は何か？
  - 安全性に関する懸念（従来の暗号アルゴリズム）
    - 量子コンピュータが現実的になった時には、従来の暗号アルゴリズムは暗号技術としての要件を満たすことができなくなる。そのため、従来の暗号アルゴリズムと PQC アルゴリズムを組み合わせて利用することにより、従来の暗号アルゴリズムの安全性を量子コンピュータにも耐えうる安全性まで引き上げる
  - 安全性に関する懸念（PQC アルゴリズム）
    - PQC に完全移行した場合、PQC アルゴリズムは従来の暗号アルゴリズムと比較して量子コンピュータに耐性はあるが、安全性評価手法などが成熟していないことや、PQC そのものが長期間利用されていないことによる未知の脆弱性などのリスクが考えられる。このリスクに対応すべくハイブリッドモードでの利用によって、PQC アルゴリズムに脆弱性が発見されたとしても、現在利用している従来の暗号アルゴリズムで達成できるセキュリティレベルは保証される。
  - 運用上の懸念
    - 実社会での新しいアルゴリズム（PQC）やプロトコルの社会実装を行うと、ネットワーク上に配置されている機器が対応していないと通信できない。このような状況を回避するために「下位互換性」を実現することで古い機器で通信を行うことができる。
    - 現行の FIPS140 などの認証プログラムは従来の暗号アルゴリズムのみに対応している。一方、NIST が行っている PQC 標準化会議は PQC 単体のみを評価しているため、実際に利用しようとすると利用できる製品や環境がない状況を生み出してしまう。

- ハイブリッドモードに何を期待しているのか？
  - 上記のような背景を踏まえて、ハイブリッドモードで利用している暗号アルゴリズムのどちらかが安全性に問題があったとしても、1 つでも無事なアルゴリズムによってセキュリティが最低限担保されることへの期待ができること。
  - 標準化やソフトウェア/ハードウェアへの実装するためのバッファ期間としてのアルゴリズムの移行やシステムマイグレーションとしての役割が期待できること。

- ハイブリッドモードの適用先はどのような領域か？
  - 暗号プリミティブとしては「鍵交換」と「デジタル署名」でのハイブリッドモードでの利用が有望であると多くの組織が述べている。
    - 例示としてあげられているのが、IETF で標準化されている TLS や SSH などの従来の暗号アルゴリズムを用いて鍵交換を行っている部分に対して PQC アルゴリズムを用いたハイブリッドモード向けの拡張を行いながら既存プロトコルの仕様との互換性を意識している。
  - ハイブリッドモードでの利用が促進されることで、実際の環境で PQC が利用されるため利用時の課題や懸念事項などを洗い出すことができる。

また、今後、ハイブリッドモードは PQC が実社会で広く利用されるための移行のための手段である側面もあるため、そのハイブリッドモードによる暗号利用を可能にするための標準化動向や OSS 実装動向についても調査を行った。実際に PQC アルゴリズムやハイブリッドモードを実装した動作実験によって、正常動作しないケースは、PQC アルゴリズム単体やハイブリッドモードの違いに影響されていないことから、特定の PQC アルゴリズムに起因することが予想される。また、PQC アルゴリズム単体で動作するアルゴリズムは、実験的ではあるがハイブリッドモードでも利用できることが期待されることがわかった。

参考文献

[1] E. Crockett, C. Paquin , D. Stebi, “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH,” 19 7 2019. . Available: https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/stebila-prototyping-post-quantum.pdf.

[2] Cloud Security Alliance Quantum-Safe Security Working group, “The State of Post-Quantum Cryptography,” 23 5 2018. . Available: https://cloudsecurityalliance.org/artifacts/the-state-of-post-quantum-cryptography/.

[3] Cloud Security Alliance Quantum-Safe Security Working group, “Applied Quantum-Safe Security,” . Available: https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf.

[4] PQCRYPTO Project, “PQCRYPTO Post-Quantum Cryptography for Long-Term Security D5.2 Standardization: Final report,” 4 2018. . Available: https://pqcrypto.eu.org/deliverables/d5.2-final.pdf.

[5] S. Douglas, “Hybrid key exchange in TLS 1.3,” . Available: https://tools.ietf.org/html/draft-ietf-tls-hybrid-design-00.

[6] A. Hopkins, “Post-quantum TLS now supported in AWS KMS,” 4 11 2019. . Available: https://aws.amazon.com/jp/blogs/security/post-quantum-tls-now-supported-in-aws-kms/.

[7] Microsoft Research, “Post-Quantum TLS,” . Available: https://www.microsoft.com/en-us/research/project/post-quantum-tls/.

[8] K. Kwiatkowski , L. Valenta, “The TLS Post-Quantum Experiment,” 30 10 2019. . Available: https://blog.cloudflare.com/the-tls-post-quantum-experiment/.

[9] B. W. Joppe, C. Costello, M. Naehrig , D. Stebila, “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem,” ePrint, 2018.

[10] J. Brendel, M. Fischlin , F. Günther, “Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids,” ESORICS 2019, 2019.

[11] F. Giacon, F. Heuer , B. Poettering, “KEM Combiners,” PKC 2018, 2018.

[12] N. Bindel, J. Brendel, M. Fischlin, B. Goncalves , D. Stebila, “Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange,” PQCrypto 2019, 2019.